



⑮ **BUNDESREPUBLIK
DEUTSCHLAND**



**DEUTSCHES
PATENT- UND
MARKENAMT**

⑫ **Offenlegungsschrift**
⑩ **DE 100 46 437 A 1**

⑤ Int. Cl.⁷:
H 04 L 9/32
G 06 F 12/14

⑲ Aktenzeichen: 100 46 437.8
⑳ Anmeldetag: 20. 9. 2000
㉓ Offenlegungstag: 4. 4. 2002

DE 100 46 437 A 1

⑦① Anmelder:
Mannesmann AG, 40213 Düsseldorf, DE

⑦④ Vertreter:
Weisse und Kollegen, 42555 Velbert

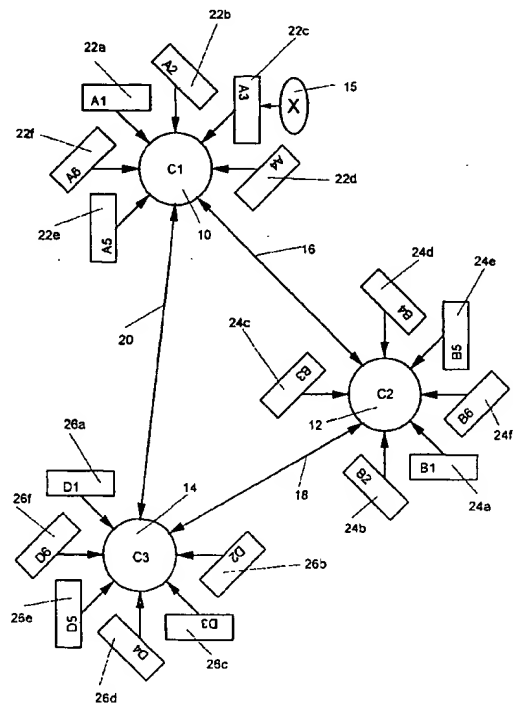
⑦② Erfinder:
Swoboda, Bernhard, 40822 Mettmann, DE;
Gerstenkorn, Wulf, 58642 Iserlohn, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

⑤④ Identifizierungsverfahren in einem Rechnernetzwerk

⑤⑦ Die Erfindung betrifft ein Verfahren zum Identifizieren einer Rechneinheit und eines Benutzers in einem Rechnernetzwerk, wobei der individuelle Seriencode einer Standard-Hardwarekomponente der Rechneinheit mit einem Programm ausgelesen und zur Identifizierung der Rechneinheit herangezogen und mit dem Benutzerkennwort kombiniert wird.



DE 100 46 437 A 1

Beschreibung

Technisches Gebiet

[0001] Die Erfindung betrifft ein Verfahren zum Identifizieren einer Rechneinheit in einem Netzwerk.

Stand der Technik

[0002] Es wird oft gefordert, daß sich ein Benutzer eines Rechners nur von einem ganz bestimmten Rechner in ein Netzwerk anmelden kann. Dabei kann es sich sowohl um ein lokales, ein Intra-Netzwerk, oder aber auch um das Internet handeln. In der Regel besteht ein solches Rechnernetzwerk aus einem oder mehreren zentralen Netzwerkrechnern, zu denen ein Benutzer mit Hilfe eines Anwenderrechners Zugang hat.

[0003] Für dieses Problem, daß sich ein Benutzer eines Rechners nur von einem ganz bestimmten Rechner in ein Netzwerk anmelden kann, existieren derzeit sogenannte "Kryptoboards", die als Hardwarekomponente in eine Rechneinheit eingebaut werden können. Auf den "Kryptoboards" ist ein digitaler Code abgespeichert, der eine eindeutige Identifizierung des Rechners bzw. des "Kryptoboards" erlaubt.

[0004] Beim Anmelden des Benutzers in das Netzwerk wird aus diesem "Kryptoboard" mittels Programm ein individueller Identifizierungscode ausgelesen. Durch die Einmaligkeit dieses Codes kann so der Rechner eindeutig in einem Netzwerk identifiziert werden. In Kombination mit der Abfrage des Benutzers und dessen Benutzerkennwortes kann auf diese Weise ein Benutzer an einen bestimmten Rechner des Netzwerkes gebunden sein. Ein Anmelden von einem anderen Rechner des Netzwerkes würde ihm verwehrt, da sowohl der korrekte Code des Kryptoboards, als auch der korrekte Benutzer und das korrekte Benutzerkennwort in Kombination vom Netzwerk gefordert wird.

[0005] Diese Kryptoboards haben den Nachteil, daß sie relativ teuer sind und zudem speziell in die Rechneinheit eingebaut werden müssen. Gegebenenfalls verbrauchen sie dann noch wertvollen Kartenplatz, der unter Umständen für andere Rechnerkomponenten benötigt wird.

Offenbarung der Erfindung

[0006] Aufgabe der Erfindung ist es daher, ein kostengünstiges Verfahren für die Identifizierung eines Benutzers in einem Rechnernetzwerk zu schaffen, bei dem sich der Benutzer immer nur von einer bestimmten Rechneinheit in das Rechnernetzwerk anmelden kann.

[0007] Erfindungsgemäß wird die Aufgabe dadurch gelöst, daß bei einem Verfahren der eingangs genannten Art der individuelle Seriencode von mindestens einer Standard-Hardwarekomponente der Rechneinheit mit einem Programm ausgelesen und zur Identifizierung der Rechneinheit herangezogen und mit dem Benutzerkennwort kombiniert wird.

[0008] Die Erfindung beruht auf dem Prinzip, daß die Hersteller von Standard-Hardwarekomponenten für Rechner bereits einen individuellen Code in die Hardware integrieren. Diese Codes werden in der Hardwarekomponente in sogenannten ROMs (Abkürzung für Read Only Memory – nur Lesespeicher) gespeichert. Grundsätzlich läßt sich jede Hardwarekomponente, bei der der individuelle Seriencode in einem ROM gespeichert ist, zur Rechneridentifizierung verwenden. Benutzerkennwort und Seriencode der Hardwarekomponente einer Rechneinheit werden einem Zentral-Netzwerkrechner mitgeteilt und dort gespeichert. Beim An-

melden ist dann immer die Kombination von Benutzerkennwort und Seriencode erforderlich, um in das Netzwerk zu gelangen. Durch geeignete Programm-Routinen können diese durch den Zentralrechner abgefragt werden. Der Vorteil bei diesem Verfahren ergibt sich dadurch, daß hierdurch kostenintensive Zusatzkomponenten, wie das Kryptoboard gespart werden. Außerdem müssen keine zusätzlichen Komponenten in den Anwenderrechner integriert werden.

[0009] Eine Netzwerkkarte ist eine besonders geeignete Hardware-Komponente, bei der der individuelle Seriencode in einem ROM der Standard-Hardwarekomponente abgelegt ist.

[0010] Zur weiteren Sicherung kann es zweckmäßig sein, daß der individuelle Seriencode mehrerer Standard-Hardwarekomponenten ausgelesen wird, um zu verhindern, daß das entsprechende Element aus der einen Rechneinheit aus- und in einen anderen Rechner eingebaut wird.

[0011] Das Programm zum Auslesen des Seriencodes kann in einer vorteilhaften Ausgestaltung der Erfindung im Hintergrund laufen, um andere Applikationen nicht zu unterbrechen, bzw. zu stören.

[0012] Es erweist sich als vorteilhaft, wenn das Programm zur Seriencode-Abfrage bereits als Bestandteil des Betriebssystems implementiert ist. Hierdurch werden zusätzliche Programme zur Abfrage nicht erforderlich. Außerdem ist es zur Standardisierung der Übergabe der entsprechenden Seriencode-Daten hilfreich.

[0013] Weitere Vorteile ergeben sich aus dem Gegenstand der Unteransprüche.

Kurze Beschreibung der Zeichnung

[0014] Fig. 1 zeigt in einer Prinzipskizze ein Netzwerk mit dem erfindungsgemäßen Verfahren zum Anmelden.

[0015] Fig. 2 zeigt eine Prinzipskizze über einen Anmeldedevorgang in ein Netzwerk mit einem erfindungsgemäßen Verfahren.

Bevorzugtes Ausführungsbeispiel

[0016] In Fig. 1 wird beispielhaft der prinzipielle Aufbau eines Netzwerkes gezeigt. Das Netzwerk besteht aus zentralen Netzwerkrechnern 10, 12 und 14 (C1, C2 und C3), die wiederum über Verbindungen 16, 18, 20 miteinander verbunden sind. Die Verbindungen können beispielsweise BNC-Kabel, aber auch Telefonleitungen sein. In diesem Ausführungsbeispiel sind nur drei zentrale Netzwerkrechner dargestellt. Es können aber beliebig viele zentrale Netzwerkrechner untereinander gekoppelt sein, wie es z. B. beim lokalen Netzwerk bis hin zum Intra- und Internet vorkommt. Um in einen der zentralen Netzwerkrechner 10, 12, 14 zu gelangen, muß ein Benutzer 15 mit der Bezeichnung X über einen der Anwenderrechner 22a bis 22f, 24a bis 24f bzw. 26a bis 26f sich im Netzwerk anmelden.

[0017] Der Benutzer 15 vertilt über ein individuelles Benutzerkennwort XY, mit dem er sich im Netzwerk als der Benutzer X zu erkennen gibt. Um zu verhindern, daß der Benutzer X sich von jedem beliebigen Anwenderrechner 22a bis 22f, 24a bis 24f bzw. 26a bis 26f bei einem der zentralen Netzwerkrechner 10, 12, 14 anmelden kann, ist sein Benutzerkennwort XY beispielsweise an den Seriencode (A3) der Netzwerkkarte des Anwenderrechners 22c gekoppelt.

[0018] Der von dem Hersteller vergebene Seriencode der Netzwerkkarte – auch MAC-Adresse (Media Access Control – Adresse/Medium Zugriffskontrolladresse) genannt – ist weltweit eindeutig. Der Code hat in der Regel eine digitale Struktur, beispielsweise mit Hexadezimalcode, der aus

den Zeichen 0-9 und A-F besteht. Dieser Seriencode dient derzeit zur Identifikation der Netzwerkkarte in einem Netzwerk und wird insbesondere als Grundlage für die Vergabe einer IP-Adresse (Internet Protokoll Adresse) verwendet.

[0019] Mit Fig. 2 soll in einem möglichen Beispiel der erlaubte Zugriff von einem der Anwenderrechner 22a-26f auf einen der zentralen Netzwerkrechner 10, 12, 14 verdeutlicht werden.

[0020] Wenn ein Benutzer 15 sich erstmalig in dem Netzwerk anmelden will, dann kennt das Netzwerk bzw. der zentrale Netzwerkrechner 10 weder den Benutzer, noch den Rechner, von dem er sich anmeldet. Es muß dem zentralen Netzwerkrechner 10 somit zunächst mitgeteilt werden, welcher Benutzer 15 und von welchem Anwenderrechner 22c er sich anmeldet. Wenn der Benutzer beim zentralen Netzwerkrechner als Benutzer eingerichtet ist, wird der Benutzer beim Anmelden durch den Zentralrechner identifiziert.

[0021] In vorliegendem Ausführungsbeispiel hat sich der Benutzer X von dem Anwenderrechner 22c bei dem zentralen Netzwerkrechner 10 angemeldet. Die Schritte, die zur Anmeldung zum zentralen Netzwerkrechner 10 erforderlich sind, werden von links nach rechts durch die Pfeile 27a bis 27e zwischen dem Netzwerkrechner 10 und dem Anwenderrechner 22c symbolisiert.

[0022] Für das Anmelden – Pfeil 27a – und Arbeiten im Internet bzw. im Intranet kann ein sogenannter "Browser" 28 verwendet werden. Der Browser 28 (auch: WEB-Browser) ist ein Programm, welches Inter- bzw. Intranetseiten darstellen kann. Internetseiten werden dazu als HTML-Code (Abkürzung für "hypertext markup language", deutsch: "Hypertext-Auszeichnungssprache") auf einem der Zentral-Netzwerkrechner 10, 12, 14 abgelegt. Der Browser 28 läuft auf dem Anwenderrechner 22c und kann diesen HTML-Code in Text und Graphik umwandeln.

[0023] Häufig werden die zentralen Netzwerkrechner 10, 12, 14 auch Verteilerrechner, Server oder Provider genannt. Durch Aufruf einer speziellen Seite mittels des Browsers 28 wird neben dem HTML-Code der Seite auch eine "Java"-Applikation (auch: Java-Applet) von dem zentralen Netzwerkrechner 10 in den Anwenderrechner 22c geladen. Die "Java"-Applikation ist ein Programm in der Programmiersprache Java, mit der der Browser 28 bzw. hierüber der Anwenderrechner 22c gesteuert werden kann.

[0024] Damit nicht bei jedem Aufruf einer Internetseite "irgendeine" Java-Applikation geladen wird, können die Java-Applikationen auch digital zertifiziert werden. Je nach Einstellung des Browsers 28 und je nach Zertifikat der Java-Applikation werden der Applikation entsprechende Rechte eingeräumt. Ist eine Java-Applikation, die auf lokale Ressourcen zugreift, nicht zertifiziert, so wird sie vom Browser 28 nicht ausgeführt. Dies soll verhindern, daß unzertifizierte Java-Applikationen Schaden an dem Anwenderrechner 22c ausüben. Die Java-Applikation weist daher neben dem Programm-Code insbesondere auch die Signatur eines Zertifikates und einen darin enthaltenen Prüfcode auf. Der Browser 28 vergleicht die Signatur mit einer ihm vorliegende Kopie des Zertifikats und stellt fest, ob die Java-Applikation mit dem Zertifikat signiert worden ist.

[0025] Wenn mit dem Browser 28 zum Anmelden eine HTML-Seite mit Java-Applikation auf dem zentralen Netzwerkrechner aufgerufen wird, dann sollte der Browser 28 zunächst feststellen, daß die Java-Applikation zertifiziert ist – Pfeil 27b. Die Java-Applikation fragt nun die MAC-Adresse der Netzwerkkarte – Pfeil 27d und neben dem Benutzer das Benutzerkennwort – Pfeil 27c – ab. Die MAC-Adresse 29 der Netzwerkkarte kann das Java-Programm direkt aus dem ROM der Netzwerkkarte auslesen und an den zentralen Netzwerkrechner 10 weiterleiten. Den Benutzer-

namen und das Benutzerkennwort 31 muß der Benutzer eingeben. Stimmen alle Daten mit den auf dem zentralen Netzwerkrechner 10 hinterlegten Daten überein, so hat der Benutzer Zugang zum Netzwerk.

[0026] Das Java-Programm kann im Hintergrund des Anwenderrechners 22c ablaufen, so daß der Benutzer von dem Einlesen der MAC-Adresse nichts bemerkt.

Patentansprüche

1. Verfahren zum Identifizieren einer Rechneinheit (22c) und eines Benutzers (15) in einem Rechnernetzwerk, **dadurch gekennzeichnet**, daß der individuelle Seriencode von mindestens einer Standard-Hardwarekomponente der Rechneinheit (22c) mit einem Programm ausgelesen und zur Identifizierung der Rechneinheit (22c) herangezogen und mit einem Benutzerkennwort kombiniert wird.
2. Verfahren zum Identifizieren einer Rechneinheit (22c) und eines Benutzers (15) in einem Netzwerk nach Anspruch 1, dadurch gekennzeichnet, daß der individuelle Seriencode in einem Speicher der Standard-Hardwarekomponente abgelegt ist.
3. Verfahren zum Identifizieren einer Rechneinheit (22c) und eines Benutzers (15) in einem Netzwerk nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß der individuelle Seriencode einer Netzwerkkarte ausgelesen wird.
4. Verfahren zum Identifizieren einer Rechneinheit (22c) und eines Benutzers (15) in einem Netzwerk nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der individuelle Seriencode mehrerer Standard-Hardwarekomponenten ausgelesen wird.
5. Verfahren zum Identifizieren einer Rechneinheit (22c) und eines Benutzers (15) in einem Netzwerk nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß das Programm zum Auslesen des Seriencodes im Hintergrund läuft.
6. Verfahren zum Identifizieren einer Rechneinheit (22c) und eines Benutzers (15) in einem Netzwerk nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß das Programm zur Seriencode-Abfrage eine Benutzerabfrage durchführt.
7. Verfahren zum Identifizieren einer Rechneinheit (22c) und eines Benutzers (15) in einem Netzwerk nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß das Programm zur Seriencode-Abfrage Bestandteil des Betriebssystems ist.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

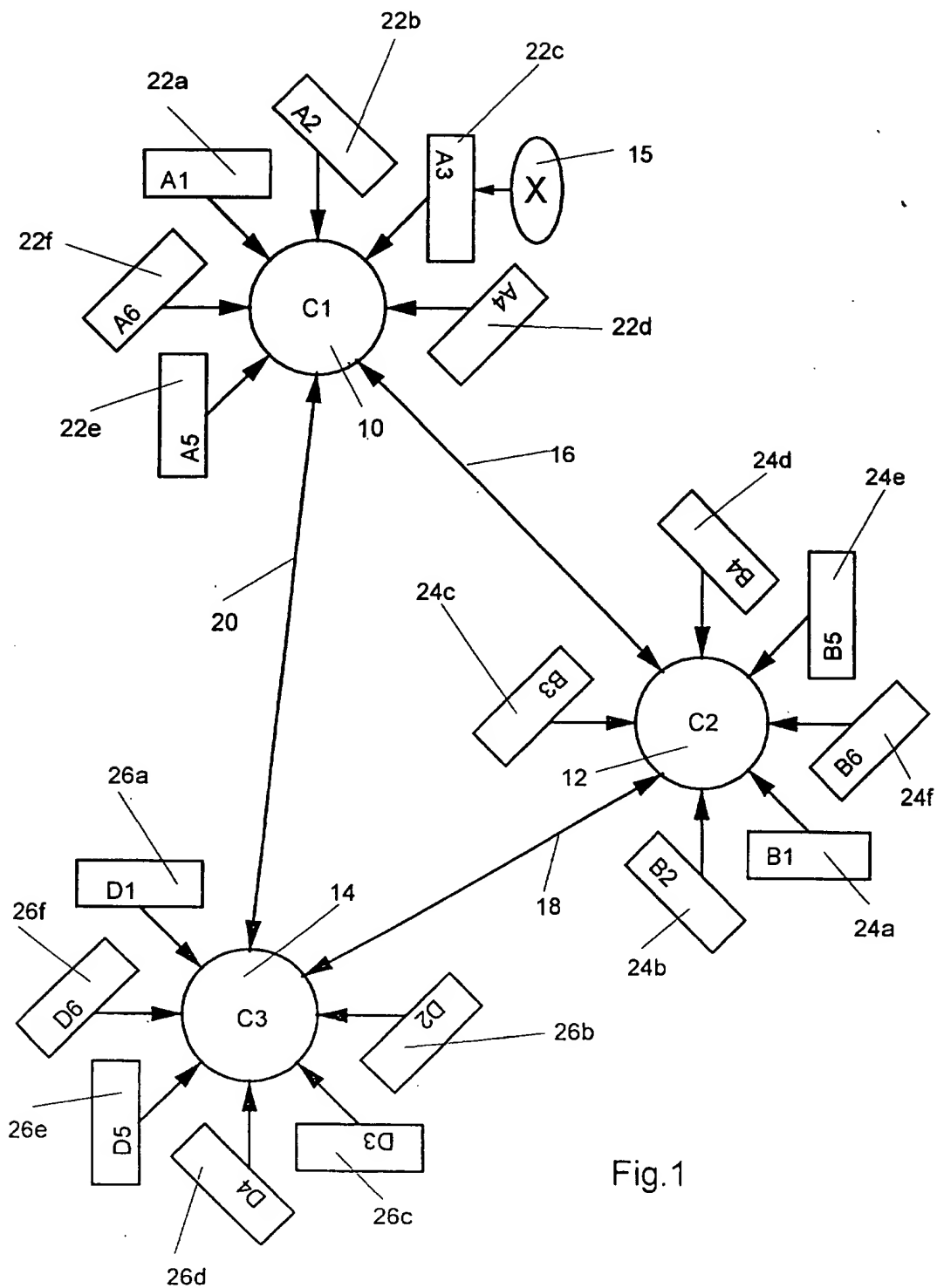


Fig.1

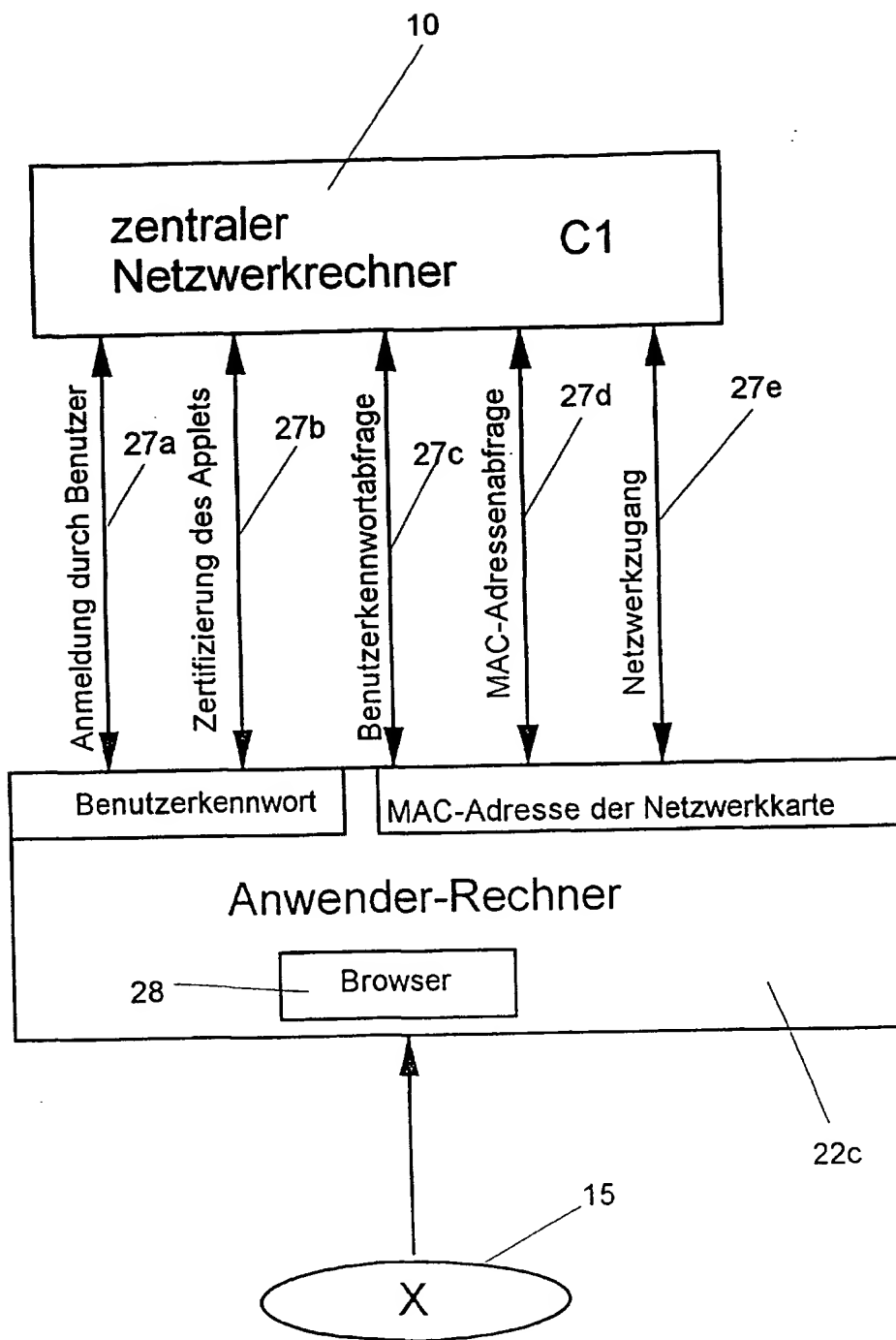


Fig. 2